REMARKS/ARGUMENTS

Claims 1–16 remain pending in the instant application, and currently stand rejected. It is believed that the remarks submitted herein below attend to each of the Examiner's rejections of claims 1–16.

Claim Rejections – 35 U.S.C. §102

Claims 1–16 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,317,766 (hereinafter, "Grover"). We respectfully disagree.

To anticipate a claim, Grover must teach every element of the claim and "the identical invention must be shown in as complete detail as contained in the ... claim." MPEP 2131 citing *Verdegaal Bros. V. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987) and *Richardson v. Suzuki Motor* Co., 868 F.2d 1226, 9 USPQ2d 1913 (Fed. Cir. 1989). Differences exist between Applicant's claimed elements and Grover such that Grover cannot be said to anticipate Applicant's invention. More specifically, Grover does not teach every element of Applicant's claims 1–16, as demonstrated herein below.

Independent Claims 1 and 15:

Independent claim 1 recites a method for encrypting programs for encrypted execution on a network having a remote host computer. Claim 15 recites a secured network for executing encrypted computer programs at a remote host computer without sharing intelligible or otherwise useful program code, computations or data associated with execution. Claims 1 and 15 share the following elements:

(a) encoding a program as a unitary matrix with n rows and n columns;

(b) encoding an input data string to the program as a vector of length n, wherein execution of the program on the input data string is realized by matrix multiplication of the unitary matrix with the vector;

(c) loading the encoded program and the encoded data string (with/on) a host computer;

(d) executing the encoded program, using the encoded data string (with/on) the host computer;

(e) communicating results from a host computer to:

a control computer (claim 1) or

a network (claim 15), and

(f) decoding the results:

- into output representative of executing the program with the data string, wherein computations and data associated with the program and data string are unintelligible and useless at the host computer (claim 1), or
- where the host computer has substantially no intelligible or otherwise useful program code, computations or data associated with execution of the program (claim 15).

Grover fails to teach each and every one of claim elements (a)–(f), and therefore cannot anticipate claims 1 and 15.

element (a): For example, claims 1 and 15 both require encoding a program as a unitary matrix with n rows and n columns. Thus, in order to anticipate the claims, Grover must also teach encoding a program as a unitary matrix. However, Grover fails to do this.

First, Grover does not teach encoding a program. Grover makes no mention of a general computer program. Rather, Grover discloses a quantum mechanical algorithm for solving certain specific problems by the repeated application of a single unitary transformation. The only encoding mentioned in Grover is applied to computational *states* of a quantum mechanical system. For example, Grover gives an example where states are encoded as "S_0, S_1...S_{N-1} (first two bits are 010, next n bits indicate the S_α state...The S_α states are the computational states". Grover col. 12, lines 1–5. A computational state is different from a program. For example, in the Grover patent, "state...means one of the N basis states in which each of the n qubits is either a 0 or a 1." Grover, col. 3, lines 38–42. Encoding such a state is different from encoding a program.

Second, because Grover does not disclose encoding a program, Grover also fails to disclose encoding a program as a unitary matrix.

Third, Grover also does not disclose encoding a program as a unitary matrix with n rows and n columns. The Examiner points to Grover col. 3, lines 5–14, stating that this passage teaches such manner of encoding. Respectfully, this is incorrect. The Examiner's cited passage merely describes the well-known Walsh-Hadamard transformation, which is a unitary matrix with 2 rows and 2 columns, performed on a two-state quantum system, or qubit. Grover recites that the Walsh-Hadamard unitary matrix $M = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ can be used when performing serial operations. See Grover col. 3, lines 43–45 and 8–10. When performing parallel operations, Grover likewise recites using "***a matrix of dimension 2" x 2"*** with values $\frac{\pm 1}{\sqrt{N}}$". Grover col. 3, lines 47–50, emphasis added. This is not a unitary matrix with n rows and n columns. On the other hand, the '402 Application clearly recites that in at least one embodiment, a program "is encoded as a unitary matrix, $U=(U_{ij})$, with n rows and n columns" Specification, p.2, ¶1, line 5.

element (b): Also contrary to the Examiner's assertion, Grover fails to teach encoding an input data string to a general program as a vector of length n, as is required in claims 1 and 15. The Grover passage cited by the Examiner (col. 3, lines 16–19) does not disclose encoding an input data string *as a vector* of length n, but shows the result of applying the 2 by 2 Walsh-Hadamard transformation *to a vector* [0, 1]. This is an example of a specific operation involving the Walsh-Hadamard transformation *on* a simple vector. See Grover col. 3, lines 13–19.

Element b, found in claims 1 and 15, also requires that "execution of the program on the input data string is realized by matrix multiplication of the unitary matrix with the vector". There is no indication within Grover of such manner of execution. First, as noted, Grover does not teach encoding an input data string as a vector of length n, and so cannot execute a program on such an input data string. Next, Grover also fails to teach program execution by matrix multiplication of the unitary matrix with the vector.

There no mention of Applicant's method of matrix multiplication within Grover. For example, Grover does not teach encoding a program "as a unitary matrix, $U=(U_{ij})$,

with n rows and n columns, such that the execution of the program on a dataset is realized by matrix multiplication of the matrix U with the vector of input data bits." Specification, p.2, ¶1, lines 5–7.

element (c): Grover also fails to teach loading such an encoded program and such an encoded data string (with/on) a host computer. The Examiner states that such element is disclosed at col. 3, lines 38–53. Respectfully, this is incorrect. As noted above with respect to element (a), the cited passage describes a special class of specific unitary matrices which have entries $\frac{\pm 1}{\sqrt{N}}$. Grover indicates that "the M transformation," or Walsh-Hadamard transformation, see equation (1), Grover col. 3, lines 6–10, "can be implemented for a single bit (i.e., for a serial arithmetic computer) with classical hardware." Grover col. 3, lines 54–56. Applying a well-known transformation via hardware is different from loading Applicant's encoded program and encoded data string; furthermore, there is no indication of how such loading might be accomplished in Grover's quantum mechanical system.

element (d): The Examiner points to the same section from Grover (col. 3, lines 38–53) in an attempt to show anticipation of element (d): executing an encoded program, using the encoded data string, on the host computer. Respectfully, the passage cited by the Examiner says nothing about executing a program using an encoded data string, in the context of a program encoded as a unitary matrix with n rows and n columns. Grover nowhere discloses such execution, especially not in the manner conveyed in the '402 application. See for example Specification p. 6, ¶2–¶3.

element (e): The Examiner again references Grover col. 3, lines 38–53 in an attempt to show Applicant's claim element (e). We have shown that this passage does not disclose elements (a)–(d), above. The passage therefore cannot disclose element (e) in the context of prior elements (a)–(d). Furthermore, Grover's only hint at a network is an indication that "words in a quantum computer can be processed serially or in parallel." Grover col. 3, lines 42–43. There is no teaching of communicating results (especially not results of executing Applicant's encoded program) from a host computer to any network, as in element (e) of claim 15. Grover is also silent as to a control computer, as in element (e) of claim 1.

element (f): Claims 1 and 15 also require decoding results. Claim particularly recites decoding results into output representative of executing the program with the data string, wherein computations and data associated with the program and data string are unintelligible and useless at the host computer. The Examiner contends that Grover discloses this step at col. 4, lines 30–63. We must disagree. This passage describes selective inversion of the phase of the amplitude of selected quantum states of a quantum register, for example as may be utilized with a series of transform elements to reach a desired result. See Grover col. 7, line 17–col. 8, line 4. It does not disclose, either explicitly or implicitly, the step of decoding results of computations and data that are otherwise unintelligible and useless at a host computer.

Grover is completely silent as to any computation or data that would be unintelligible to a host computer, notably because Grover teaches against such unintelligible data or computations. Grover recites an element 201, upon which a unitary transformation operation is performed. Grover specifies that, following a prescribed number of repetitions, the desired result of such operations "can be utilized immediately", Grover col. 8, lines 2-3, by the machine where such operation the operations are taking place. See Grover col. 7, line 36 – col. 8, line 4; FIG. 3. Grover cannot and does not teach Applicant's element of decoding results, at least because Grover does not teach computations and data that are otherwise unintelligible and useless at a host computer.

In addition, independent claim 15 particularly recites communicating results to the control computer for decoding, the host computer having substantially no intelligible or otherwise useful program code, computations or data associated with execution of the program. Again, neither the cited passage nor any other section of Grover recites such a limitation.

Because Grover fails to teach claim elements (a)–(f), claims 1 and 15 are not anticipated. Withdrawal of the Examiner's rejection is respectfully requested.

Dependent Claims 2–14:

Claims 2–14 depend from claim 1, either directly or through intervening claims. Claims 2–14 are therefore not anticipated by Grover, for at least the reasons laid out

herein above. However, we submit that these claims are further allowable over Grover, for additional reasons exemplified herein below.

Claims 2–4: The Examiner applies Grover col. 8 line 58– col. 9, line 18 in an attempt to show anticipation of claims 2–4. However, this passage fails to recite any of:

- converting a program to a unitary matrix multiplication (claim 2);
- converting the program to a unitary matrix multiplication U such that $U \in U_n$ for some integer n, where U_n represents a group of unitary matrices of size n (claim 3), or
- generating two independent identically distributed unitary matrices X, Y from the uniform probability distribution over U_n determined by the Haar distribution (claim 4).

The passage cited by the Examiner describes the repeated operation of a specific unitary matrix. There is no mention whatsoever of program conversion to a unitary matrix multiplication. Grover is also silent as to generating two independent identically distributed unitary matrices from any probability distribution. In particular, Grover does not mention the Haar distribution, at all. Withdrawal of the Examiner's rejection is respectfully requested.

Claims 5 and 6: The Examiner states that Grover col. 9, lines 14–19 discloses the following:

- computing U' as XUY* and communicating U' to a remote host computer over the network (claim 5), and
- converting an input data string to a vector b (claim 6).

Again, we must disagree. The cited passage simplifies the operations in equation (12) of Grover. See Grover col. 9, lines 10–16. This has nothing to do with encoding a program, U, by computing U'=XUY*. In particular, the passage is irrelevant to such computation where X and Y are random unitary matrices, as in at least one embodiment of the '402 Application. See Specification page 3, ¶3 –¶1, page 4.

The cited Grover passage is also inapplicable to claim 6, at least because it makes absolutely no mention of any kind of input data. As previously noted, Grover does not teach converting an input data string to a vector, at all.

For at least the reasons given herein above, Grover does not anticipate claims 5 and 6. We therefore respectfully request withdrawal of the Examiner's rejection.

Claim 7: Grover also fails to anticipate claim 7. Claim 7 requires the steps of encoding input data strings by:

- computing b' as Yb, and
- communicating b' to the remote host over the network.

Grover discloses no such steps for encoding input data strings. In particular, the passage cited by the Examiner (Grover col. 11, lines 16-53) describes estimating the convergence rate of a specific iteration that is key to the Grover patent. The cited passage does not describe or even mention encoding input data strings. Withdrawal of the Examiner's rejection is respectfully requested.

Claims 8–9: The Examiner contends that Grover col. 12, line 51–col. 13, line 22 teaches:

- executing encoded data strings including the steps of (a) computing the product of XUY* and Yb and (b) communicating results to the network (claim 8), and
- decoding the results into output, including computing X*XUb, external of the host computer, to determine the multiplication of Ub as desired output of the program, wherein XUY* and Yb is (XUb) and X*XUb is obtained by matrix multiplication X*(XUb) (claim 9).

Respectfully, Grover does not teach or even mention elements (a), (b) of claim 8, nor does Grover teach decoding the results into output as recited in claim 9. The passage cited by the Examiner describes the measurement procedure when Grover's computation is repeated multiple times, to estimate μ. See Grover col. 12, line 51–col. 13, line 22.

Withdrawal of the Examiner's rejections of claims 8 and 9 is therefore respectfully requested.

Claim 10: Grover col. 3, lines 38–53 is again cited. This time, the Examiner states that the passage discloses the claim 10 limitation of "decoding comprising decrypting at a control computer connected to a network and a host computer." We respectfully disagree. As noted with respect to claim 1, the cited Grover passage describes a special class of specific unitary matrices which have entries $\frac{\pm 1}{\sqrt{N}}$. Grover makes brief mention of parallel processing words, see col. 3, lines 45-51; however, this is not decoding or decrypting at a control computer connected with a network. As is known in the art, parallel processing of words within a computer is done using parallel circuits, not networks. As is further known in the art, parallel processing of words is done to improve efficiency, not to encrypt or decrypt data.

Furthermore, Grover makes no mention of decoding or decrypting, at a host computer or elsewhere, and especially not decoding results "into output representative of executing the program with the data string", where "computations and data associated with the program and data string are unintelligible and useless at the host computer" (limitations inherited from claim 1). Claim 10 is not anticipated; withdrawal of the Examiner's rejection is requested.

Claims 11–13: The Examiner next contends that this same passage (Grover col. 3, lines 38–53) suggests the following limitations of claims 11–13:

- a network comprising the Internet (claim 11);
- a network comprising a virtual private network (claim 12), and
- a network comprising a local area network (LAN) (claim 13).

Respectfully, Grover lacks any reference to a network comprising the Internet, a virtual private network or a LAN. Thus, no anticipation can be found with respect to claims 11–13.

Furthermore, even if Grover did "suggest" these limitations, such a suggestion would be insufficient to alone render an anticipation rejection. Pursuant MPEP §706.02(V):

> "for anticipation under 35 U.S.C. §102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be **inherently present**." (emphasis added)

Regarding inherency, MPEP §2112 states:

> "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic **necessarily** flows from the teachings of the applied prior art. *Ex parte Levy*, 17 USPQ2D 1461, 1464 (Bd. Pat. App. & Inter. 1990)."

In stating that Grover suggests the features of claims 10–13, we contend that the Examiner admits that these features are not directly taught. We agree that Grover does not teach these features. Per MPEP §706.02(V), features not directly taught must be inherently present. The Examiner has not provided any factual or technical reasoning to support an inherently present Internet, virtual private or LAN network, as required per MPEP §2112, thus, inherency is not established and there is no anticipation of "suggested" features of claims 11–13. Withdrawal of the rejection of claims 11-13 is respectfully requested.

Claim 14: Claim 14 requires embedding one or more constants into an input data string or program, prior to encoding, to detect incorrect execution or data tampering. In one embodiment, "This can be accomplished by appending a trailing 1, as $\begin{bmatrix} b \\ 1 \end{bmatrix}$, to the input data vector b and embedding U into an (n+1) by (n+1) unitary as $\begin{bmatrix} U & 0 \\ 0 & 1 \end{bmatrix}$ so that the correct output is $\begin{bmatrix} Ub \\ 1 \end{bmatrix}$. Any change to $X\begin{bmatrix} Ub \\ 1 \end{bmatrix}$ either through error or malicious

tampering will result in a decoded answer that will not have exactly 1 as the trailing entry of the decoded output vector $\begin{bmatrix} Ub \\ 1 \end{bmatrix}$." Specification, p. 5, ¶2, lines 3–7.

Grover does not teach such embedding. The passage cited by the Examiner at col. 13, lines 22–47 proposes that the ideas in the Grover patent can be used to accelerate a general quantum mechanical algorithm. It does not disclose the use of constants in an input data string or program, especially not for the detection of incorrect execution or tampering.

Grover does not teach claim 14. We therefore respectfully request withdrawal of the Examiner's rejection.

Dependent Claim 16:

Claim 16 depends from claim 15, thus benefiting from like arguments. See the arguments presented in support of claim 15, above. Furthermore, Grover does not teach a control computer that embeds one or more constants into a unitary matrix or data string, wherein the results from the host computer indicate tampering or incorrect execution of the encoded program. The Examiner's cited passage does not teach such limitations, but rather describes the repeated operation of a specific unitary matrix. See Grover col. 8, line 58–col. 9, line 18; see also arguments in support of claims 2–4, above. Withdrawal of the Examiner's rejection of claim 16 is respectfully requested.

CONCLUSION

Claims 1–16 remain pending in the '402 Application. In view of the above remarks, Applicant respectfully requests allowance of all pending claims.

The due date for submission of this response with a Petition for One Month Extension of Time fell upon a Sunday (September 4, 2005), which was followed by the Labor Day Holiday (Monday, September 5). This response is therefore timely submitted with said Petition today, Tuesday September 6, 2005. Per 37 C.F.R. §1.7, *"When the day, or the last day fixed by statute or by or under this part for taking any action or*

paying any fee in the United States Patent and Trademark Office falls on Saturday, Sunday, or on a Federal holiday within the District of Columbia, the action may be taken, or the fee paid, on the next succeeding business day which is not a Saturday, Sunday, or a Federal holiday."

The aforementioned Petition for One Month Extension of Time is submitted herewith, along authorization to charge the required fee of $60 to Deposit Account No. 12-0600. Given the weekend and holiday, this serves to extend the period for reply up to, and including, September 6, 2005. It is believed that no further fees are due; however, if any additional fee is deemed necessary in connection with this Response, please charge Deposit Account No. 12–0600. Should any issues remain, the Examiner is encouraged to telephone the undersigned attorney.

Respectfully submitted,

LATHROP & GAGE L.C.

Date: 6 Sep 2005

By: Curtis A. Vock

Curtis A. Vock, Reg. No. 38,356
Lathrop & Gage L.C.
4845 Pearl East Circle
Suite 300
Boulder, CO 80301
Tele: (720) 931-3011
Fax: (720) 931-3001